AMENDMENTS TO THE SPECIFICATION:

Please amend the specification as follows:

Please replace the paragraph beginning at page 7, line 26, which starts with "This cryptographic communication" with the following amended paragraph:

This cryptographic communication system comprises a key recovery agent 3, certificate authority 2, and approver 4 to allow recovering a session key or user's private key in cryptographic communications between users [[1]] 1a and 1b. The ~~user 1~~ users 1a, 1b, and 1c, key recovery agent 3, certificate authority 2, and approver 4 can communicate with each other via a network (e.g., the Internet) made up of a public network.

Please replace the paragraph beginning at page 8, line 7, which starts with "FIG. 2 is a block diagram" with the following amended paragraph:

FIG. 2 is a block diagram showing the hardware arrangement of an apparatus constructing the ~~user 1~~ users 1a, 1b, and 1c, key recovery agent 3, certificate authority (key recovery center) 2, or approver 4.

Please replace the paragraph beginning at page 8, line 11, which starts with "An apparatus 11 made up" with the following paragraph:

An apparatus 11 made up of the ~~user 1~~ users 1a, 1b, and 1c, key recovery agent 3, certificate authority 2, ~~or~~ and approver 4 has a hardware computer system made up of a CPU 12, controller 13, memory 14, communication device 15, display 16, keyboard 17, printer 18, and data bus 19.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

Please replace the paragraph beginning at page 8, line 16, which starts with " Of these components" with the following amended paragraph:

Of these components, the memory 14 includes both a so-called main memory (e.g., a RAM) and a secondary memory (e.g., a hard disk). The functions to be performed by the ~~user 1~~ users 1a, 1b, and 1c, key recovery agent 3, the certificate authority 2, or approver 4 are implemented by programs loaded on the main memory and control of the CPU 12 based on these programs. More specifically, the ~~user 1~~ users 1a, 1b, and 1c, key recovery agent 3, the certificate authority 2 and approver 4 have different software arrangements. The detailed contents of the functions performed by a combination of hardware and software will be described later with reference to the operational descriptions and flow charts.

Please replace the paragraph beginning at page 9, line 2, which starts with "A communication message" with the following amended paragraph:

A communication message, various certificates, public key, various information lists, and the like are stored in part of the second memory of the memory 14 in correspondence with the ~~user 1~~ users 1a, 1b, and 1c, key recovery agent 3, certificate authority 2 and approver 4, respectively. The storage data is used to perform the respective functions.

Please replace the paragraph beginning at page 9, line 12, which starts with "The user 1, key recovery" with the following amended paragraph:

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

The ~~user 1~~ users 1a, 1b, and 1c, key recovery agent 3, certificate authority 2, or approver 4 will be described below.

Please replace the paragraph beginning at page 9, lines 14, which starts with "The user 1 represents" with the following amended paragraph:

In FIG. 1, the ~~The~~ user [[1]] 1a represents a sender who sends a cipher message (cryptographic communication), the user 1b represents a receiver who receives the cipher message, ~~or~~ and the user 1c represents an authentic third party who intercepts the encrypted message. ~~In FIG. 1, the user 1 (#1), user 1 (#2), and user 1 (#3) are defined as the sender, receiver, and authorized third party, respectively.~~ The ~~user 1~~ users 1a, 1b, and 1c have ~~has~~ all functions necessary for the sender, receiver, and authorized third party and selectively ~~serves~~ serve as one of them depending on the situation.

Please replace the paragraph beginning at page 9, line 24, which starts with "More specifically, the user 1" with the following amended paragraph:

More specifically, the ~~user 1~~ users 1a, 1b, and 1c have their ~~has his~~ own public and private keys, and ~~has~~ have a function of registering the key recovery agent 3 cipher message preparation function, message transmission/reception function, cipher message decryption function, and key recovery request/recovery function. Note that the apparatus 11 in FIG. 2 constructs the encryption apparatus of the ~~user 1~~ users 1a, 1b, and 1c.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

Please replace the paragraph beginning at page 10, line 5, which starts with "The key recovery agent 3" with the following amended paragraph:

The key recovery agent 3 has its own public and private keys, and decrypts the received key recovery field with its own private key in response to a request from the registered ~~user 1~~ users 1a, 1b, or 1c and sends back the decrypted recovery field. In doing these processes, the key recovery agent 3 checks the registration signature of the approver 4. There can be a large number of key recovery agents 3. When a given key recovery agent is registered in the certificate authority 2, this agent serves as the key recovery agent 3 in this embodiment. Key recovery agents 3 (#1) through 3 (#n) are available in this embodiment.

Please replace the paragraph beginning at page 10, line 17, which starts with "The certificate authority 2" with the following amended paragraph:

The certificate authority 2 has its own public a private keys and gives signatures (certificate) to each ~~user 1~~ users 1a, 1b, or 1c, key recovery agent 3, and approver 4 to issue various certificates. The certificate authority 2 discloses these pieces of information to the user 1 and the like.

Please replace the paragraph beginning at page 10, line 23, which starts with "The approver 4 issues" with the following amended paragraph:

The approver 4 issues an approval to the ~~user 1~~ users 1a, 1b, or 1c when ~~this user 1~~ one of users 1a, 1b, or 1c performs registration in the key recovery agent and makes a key recovery request. There can be a large number of approvers 4.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

Approvers 4 (#1) through 4 (#n) are available in this embodiment. The ~~user 1~~ users 1a, 1b, or 1c can receive one approval from a plurality of approvers 4. In this case, a representative approver is given.

Please replace the paragraph beginning at page 12, line 9, which starts with "This key recovery agent 3" with the following amended paragraph:

This key recovery agent 3 is registered in the user/approver/key recovery agent registration information table in the certificate authority 2. The contents of this registration information table are disclosed to the ~~user 1~~ users 1a, 1b, and/or 1c. The key recovery agent 3 means the agent registered in the certificate authority 2.

Please replace the paragraph beginning at page 12, line 17, which starts with "The user 1 who wants" with the following amended paragraph:

The user [[1]] 1a who wants to send a message selects a key recovery agent and registers the selected key recovery agent in the certificate authority 2.

Please replace the paragraph beginning at page 12, line 22, which starts with "Assume that the user 1" with the following amended paragraph:

Assume that the user ~~1 (#1)~~ 1a in FIG. 1 registers a key recovery agent.

Please replace the paragraph beginning at page 12, line 24, which starts with "In subscription to one" with the following amended paragraph:

In subscription to one or a plurality of key recovery agents 3, the user ~~1 (#1)~~ 1a sends a key recovery agent registration application 18 to the approver 4 (t1 in FIG. 4; c in FIG. 1).

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

Please replace the paragraph beginning at page 13, line 1, which starts with "The user 1 may request" with the following amended paragraph:

The user [[1]] 1a may request an approval to one approver 4 or approvals to a plurality of approvers 4 in order to improve the safety pertaining to the key recovery. To request approvals to the plurality of approvers 4, the user [[1]] 1a sends a registration application to only a representative approver. (t1 in FIG. 4).

Please replace the paragraph beginning at page 13, line 7, which starts with "The representative approver transmits" with the following amended paragraph:

The representative approver transmits the registration application to each approver 4, and each approver 4 checks the contents of the key recovery agent registration application and gives a signature (e.g., using a multiple signature scheme). The application is finally returned to the representative approver. A key recovery agent registration approval is transmitted from the representative approver to the user ~~1 (#1)~~ 1a (t2 in FIG. 4; d in FIG. 1).

Please replace the paragraph beginning at page 13, line 16, which starts with "The user 1 (#1) sends" with the following amended paragraph:

The user ~~1 (#1)~~ 1a sends a subscription application with the key recovery agent registration approval acquired from the approvers 4 to each key recovery agent 3 that the user ~~1 (#1)~~ 1a wants to register (t3 in FIG. 4; e in FIG. 1). Note that the number of key recovery agents that the user [[1]] 1a wants to register may be one, but the user [[1]] 1a registers a plurality of key recovery agents 3 in principle.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

Please replace the paragraph beginning at page 13, line 24, which starts with "Upon receiving the" with the following amended paragraph:

A5

Upon receiving the registration approval, each key recovery agent 3 checks the signatures of the approvers 4 in the key recovery agent registration approval and adds its own signature to this approval. Each key recovery agent 3 issues a key recovery agent registration certificate to the user ~~1 (#1)~~ 1a (t4 in FIG. 4; f in FIG. 1).

Please replace the paragraph beginning at page 14, line 8, which starts with "The user 1 (#1) requests" with the following amended paragraph:

A6

The user ~~1 (#1)~~ 1a requests the certificate authority 2 to issue a registered key recovery agent list certificate with the key recovery agent registration certificates acquired from the agents 3 (t6 in FIG. 4; g in FIG. 1).

Please replace the paragraph beginning at page 14, line 13, which starts with "The certificate authority 2" with the following amended paragraph:

The certificate authority 2 checks the signatures of the key recovery agents 4 on the key recovery agent registration certificates and adds its own signature. The certificate authority 2 issues a registered key recovery agent list certificate to the user ~~1 (#1)~~ 1a (t7 in FIG. 4; h in FIG. 1).

Please replace the paragraph beginning at page 14, line 19, which starts with "The key recovery agents" with the following amended paragraph:

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

The key recovery agents 3 listed up in this agent list are the registered key recovery agents 3 of the user ~~1 (#1)~~ 1a. The key recovery field of the user ~~1 (#1)~~ 1a can be decrypted using the private keys of these agents 3.

Please replace the paragraph beginning at page 15, line 3, which starts with "Referring to FIG. 5" with the following amended paragraph:

Referring to FIG. 5, the registration information table 21 has public keys 23 with signatures approved as the public keys of the ~~user 1~~ users 1a, 1b, and 1c, and a user registered agent list 24 in correspondence with user IDs (identification information) 22 of the ~~user 1~~ users 1a, 1b, and 1c, approvers 4, or key recovery agents 3.

Please replace the paragraph beginning at page 15, line 9, which starts with "The public key 23" with the following amended paragraph:

The public key 23 with a signature represents that this key is a public key of the ~~user 1~~ users 1a, 1b, or 1c, or the like, which is approved by the certificate authority. This public key 23 is issued to a requester for this information in the form of a public key certificate.

Please replace the paragraph beginning at page 15, line 19, which starts with "The contents of the" with the following amended paragraph:

The contents of the registration information table 21 are open to the public, and the ~~user 1~~ users 1a, 1b, and 1c or agent 3 can know the table contents as if it finds out a telephone number in a telephone directory. The agent 3 registered in the table 21

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

registers its own public key in the certificate authority 2. Such a key may be listed on the table 21.

Please replace the paragraph beginning at page 15, line 27, which starts with "A process for actually" with the following amended paragraph:

A process for actually exchanging a cipher message between the users [[1]] 1a and 1b who have registered the agents will be described below. In this case, the user ~~1 (#1)~~ 1a serves as a sender, and the user ~~1 (#2)~~ 1b serves as a receiver. Note that the user 1 (#2) have already registered the agents in the process shown in FIG. 4.

Please replace the paragraph beginning at page 16, line 11, which starts with "The user 1 (#1) serving" with the following amended paragraph:

The user ~~1 (#1)~~ 1a serving as a sender (to be simply referred to as a sender hereinafter) inquires of the certificate authority 2 the receiver's public keys and the registered key recovery agent list in order to obtain the information of the key recovery agents 3 (v1 in FIG. 6; i in FIG. 7).

Please replace the paragraph beginning at page 18, line 11, which starts with "The cipher message 31" with the following amended paragraph:

The cipher message 31 constructed as described above is transmitted from the sender (user ~~1 (#1)~~ 1a) to the receiver (user ~~1 (#2)~~ 1b) (v4 in FIG. 6; k in FIG. 7).

Please replace the paragraph beginning at page 18, line 21, which starts with "Decrypting the cipher message" with the following amended paragraph:

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

Q12

Decrypting the cipher message normally as in step v5 of FIG. 6 suffers no problem. A recovery process will be described when the user [[1]] 1a or 1b loses a session key.

Please replace the paragraph beginning at page 19, line 2, which starts with "Assume that the user 1" with the following amended paragraph:

Q13

Assume that the user [[1]] 1a or 1b who requests key recovery has, in advance, information (e.g., an ID) pertaining to the key recovery agent 3 capable of recovering a key recovery field serving as a recovery target. In this case, ~~the~~ a user [[1]] is a message sender (user ~~1 (#1)~~ 1a) or message receiver (user ~~1 (#2)~~ 1b).

Please replace the paragraph beginning at page 19, line 10, which starts with "When the user 1 (#2)" with the following amended paragraph:

Q14

When the user ~~1 (#2)~~ 1b loses the session key (w1 in FIG. 9), he sends a key recovery approval application to the approvers 4 (w2 in FIG. 9; 1 in FIG. 10).

Please replace the paragraph beginning at page 19, line 13, which starts with "The approvers 4 check" with the following amended paragraph:

The approvers 4 check the key recovery approval application and add signatures (e.g., using a multiple signature scheme). A representative approver sends back a key recovery approval to the user ~~1 (#2)~~ 1b (w3 in FIG. 9; m in FIG. 10).

Please replace the paragraph beginning at page 19, line 18, which starts with "The user 1 (#2) extracts" with the following amended paragraph:

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

a14

The user ~~1 (#2)~~ 1b extracts the key recovery field 33 or 34 from the cipher message 32 and prepares a message to each key recovery agent 3 designated in the extracted key recovery field (w4 in FIG. 9).

Please replace the paragraph beginning at page 20, line 5, which starts with "The user 1 (#2) transmits" with the following amended paragraph:

a15

The user ~~1 (#2)~~ 1b transmits the message 41 containing the approval 42 and recovery field 43 to each key recovery agent 3 (w5 in FIG. 9; n in FIG. 10).

Please replace the paragraph beginning at page 20, line 14, which starts with "Upon checking the approval 42" with the following amended paragraph:

a16

Upon checking the approval 42, the key recovery agent 3 decrypts the key recovery field 43 with its own private key to recover the session key pieces (w7 in FIG. 9). The recovered pieces are encrypted with the encryption key [SK'] and transmitted from the agent 3 to the user ~~1 (#2)~~ 1b (w7 in FIG. 9; o in FIG. 10). The key recovery agent 3 receives a session key from athe agent or it recovers the session key from the pieces (w8 in Fig. 9).

Please replace the paragraph beginning at page 20, line 20, which starts with "Upon receiving these session" with the following amended paragraph:

Upon receiving these session key pieces, the user ~~1 (#2)~~ 1b decrypts with the decryption key [SK'] the encrypted session key transmitted from each key recovery agent 3. The user ~~1 (#2)~~ 1b then recovers the original session pieces using, e.g., a

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

Langragean interpolation polynomial on the basis of the decrypted session key pieces (w7 in FIG. 9).

Please replace the paragraph beginning at page 21, line 7, which starts with "Operation will be described" with the following amended paragraph:

Operation will be described when ~~the~~ a user [[1]] who requests key recovery does not have information (e.g., an ID) pertaining to the key recovery agent 3 capable of recovering a key recovery field serving as a recovery target. In this case, ~~the~~ a user [[1]] may be an authentic third party (user ~~1 (#1)~~ 1c).

Please replace the paragraph beginning at page 21, line 18, which starts with "The user 1 (#3) inquires" with the following amended paragraph:

The user ~~1 (#3)~~ 1c inquires of the certificate authority 2 the sender's or receiver's public key and the registered key recovery agent list (x1 in FIG. 12).

Please replace the paragraph beginning at page 21, line 21, which starts with "The certificate authority 2" with the following amended paragraph:

The certificate authority 2 prepares a sender's or a receiver's public key certificate and registered key recovery agent list certificate from the contents of the registration information table 21 and transmits them to the user [[1]] 1c. The user ~~1 (#3)~~ 1c receives them (x2 in FIG. 12). This process corresponds to user's operation for finding a telephone number in a telephone directory (registration information table 21) arranged in the certificate authority 2.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

Please replace the paragraph beginning at page 22, line 3, which starts with "The user 1 (#3) requests" with the following amended paragraph:

The user ~~1 (#3)~~ 1c requests approvals for key recovery to the approvers 4 (p and q in FIG. 1) and sends the approvals together with the key recovery field serving as the recovery target to the key recovery agents 3 and then obtains the recovery pieces (r and s in FIG. 1). The user ~~1 (#3)~~ 1c recovers the session key. This process is the same as in steps ww (w2 through w8) in FIG. 9, and a detailed description thereof will be omitted (X3 in Fig. 2).

Please replace the paragraph beginning at page 22, line 13, which starts with "The recovery of the session" with the following amended paragraph:

The recovery of the session key itself contained in cryptographic communication has been described above. Other keys may be recovered using the system of this embodiment. An example of other keys is a private key (user's private key) used by the user [[1]] 1a, and its recovery process will be described below. In this case, this embodiment serves as a key recovery system.

Please replace the paragraph beginning at page 22, line 23, which starts with "The user 1 (#1) encrypts its own private key" with the following amended paragraph:

The user ~~1 (#1)~~ 1a encrypts its own private key with the public key of the key recovery agent 3 (when the number of registered agents is one) or expands the private key into pieces (when the number of registered agents are many; this will apply to the following description). The user ~~1 (#1)~~ 1a generates user's private key recovery fields

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP
1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

obtained by encrypting the respective pieces with the public keys of different key recovery agents and stores them in the memory of the user as the private key backup. Such a user's private key recovery field corresponds to the sender's or receiver's key recovery field.

Please replace the paragraph beginning at page 23, line 8, which starts with "The user's private key recovery" with the following amended paragraph:

The user's private key recovery field stores the key recovery agent IDs and data of private keys encrypted with the public keys of the key recovery agents or data of encrypted private key pieces. The number of pairs of storage data is equal to the number of key recovery agents. When a private key is lost or destroyed due to some reason, and the user cannot recover the key, the user ~~1 (#1)~~ 1a sends a user's private key recovery approval application to the approvers 4 (t in FIG. 14). Each approver 4 checks the user's private key recovery approval application and gives its signature (e.g., using a multiple signature scheme). The final approver (representative approver) transmits a user's private key recovery approval to the user ~~1 (#1)~~ 1a (u in FIG. 13).

Please replace the paragraph beginning at page 23, line 23, which starts with "The user 1 (#1) then sends" with the following amended paragraph:

The user ~~1 (#1)~~ 1a then sends, to each key recovery agent 3, a user' private key recovery approval encrypted with the public key of each key recovery agent, a user's private key recovery field, and an encryption key used to transmit the recovered user's

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

private key or user's private key pieces (v in FIG. 13). Data transmitted at this time is like the one shown in FIG. 11.

Please replace the paragraph beginning at page 24, lines 4, which starts with "Each key recovery agent 3" with the following amended paragraph:

Each key recovery agent 3 decrypts the encrypted user's private key recovery approval, user's private key recovery field, and encryption key used to transmit the decrypted user's private key pieces (or user's private key). Each key recovery agent 3 checks the signature of the approver on the user's private key recovery approval. Each key recovery agent recovers the private key pieces (or the entire private key) using the user's private key recovery field and sends, to the user ~~1 (#1)~~ 1a, the private key pieces (or the entire private key) encrypted using the encryption key for private key piece transmission designated by the user (w in FIG. 13).

Please replace the paragraph beginning at page 24, line 17, which starts with "The user 1 (#1) decrypts" with the following amended paragraph:

The user ~~1 (#1)~~ 1a decrypts the encrypted private key pieces (or the entire private key) transmitted from each key recovery agent 3. Upon receiving the key pieces, for example, the Lagrange interpolation formula is used to recover the original private key based on the private key pieces.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com